

IN THE CLAIMS:

- 1 1. (original) A system for producing multiple-symbol randomizer sequences over  
2  $GF(2^m)$ , the system including:  
3 A. a first register for supplying an initial state, the register holding a non-zero  
4 element of  $GF(2^m)$ ;  
5 B. a first multiplier for multiplying the contents of the register by a multiplier  
6 constant that is a primitive element of  $GF(2^m)$ ; and  
7 C. first feedback means for  
8 i. supplying the products produced by the multiplier as the symbols of the  
9 randomizer sequence, and  
10 ii. supplying the symbols of the randomizer sequence to update the first  
11 register.
- 1 2. (original) The system of claim 1 further including:  
2 D. one or more second registers for holding elements of  $GF(2^m)$ ;  
3 E. one or more second multipliers for multiplying the contents of the one or more  
4 second registers by one or more multiplier constants that are elements of  $GF(2^m)$ ;  
5 F. an adder for adding the products produced by the first and second multipliers  
6 and supplying the sum to the first feedback means; and  
7 G. second feedback means to supplying the contents of the first register to update  
8 the second register.
- 1 3. (original) The system of claim 1 further including a selection means for selecting the  
2 initial state of the first register in order to produce a randomizer sequence that provides  
3 for encryption.
- 1 4. (currently amended) The system of claim 2 further including a selection means a  
2 ~~means~~ for selecting an initial state for the first register and the one or more second regis-  
3 ters.

- 1 5. (original) The system of claim 1 further including encryption means for encrypting a  
2 code word, the encryption means including:
- 3 a. selection means for selecting an initial state for use in producing the random-  
4 izer sequence;
- 5 b. means for combining the randomizer sequence with an ECC code word that is  
6 encoded in accordance with a given BCH code over  $GF(2^m)$ , the means pro-  
7 ducing a randomized code word; and
- 8 c. means for producing a key associated with the selected the initial state.

- 1 6. (original) The system of claim 5 further including a decrypting subsystem for using the  
2 key to reproduce the randomizer sequence and removing the randomizer sequence from  
3 the randomized code word to reproduce the ECC code word.

- al
- 1 7. (original) The system of claim 1 wherein the multiplier constant is selected to produce  
2 randomizer sequences that are each a predetermined minimum distance from code words  
3 of a given BCH code.

- 1 8. (original) The system of claim 6 further including means for detecting mis-  
2 synchronization, the mis-synchronization detection means including:
- 3 a. means for combining the randomizer sequence with an ECC code word that is  
4 encoded in accordance with a given BCH code over  $GF(2^m)$ , the means producing a ran-  
5 domized code word;
- 6 b. means for removing the randomizer sequence from the randomized code word  
7 to reproduce the ECC code word; and
- 8 c. a decoder for decoding the reproduced ECC code word, the decoder detecting a  
9 mis-synchronization if the number of errors in the reproduced ECC code word is greater  
10 than the number of errors that can be corrected by the given BCH code.

1 9. (original) The system of claim 7 wherein the multiplier constant is further selected  
2 from a set of multiplier constants which each produce randomizer sequences that are at  
3 least a predetermined minimum distance from code words of a given BCH code.

1 10. (original) The system of claim 9 further including a means for providing a key to se-  
2 lect the multiplier constant for a given randomizer sequence.

1 11. (original) The system of claim 2 wherein the multiplier constants are selected to pro-  
2 duce randomizer sequences that are each a predetermined minimum distance from code  
3 words of a given BCH code.

1 12. (original) The system of claim 11 further including means for detecting mis-  
2 synchronization, the mis-synchronization detection means including:

3 a. means for combining the randomizer sequence with an ECC code word that is  
4 encoded in accordance with a given BCH code over  $GF(2^m)$ , the means producing a ran-  
5 domized code word;

6 b. means for removing the randomizer sequence from the randomized code word  
7 to reproduce the ECC code word; and

8 c. a decoder for decoding the reproduced ECC code word, the decoder detecting a  
9 mis-synchronization if the number of errors in the reproduced ECC code word is greater  
10 than the number of errors that can be corrected by the given BCH code.

1 13. (original) The system of claim 12 wherein the multiplier constants are further selected  
2 from a set of multiplier constants that produce randomizer sequences that are at least a  
3 predetermined minimum distance from code words of a given BCH code.

1 14. (original) The system of claim 13 further including a means for providing a key to  
2 select the multiplier constants for a given the randomizer sequence.

1 15. (original) The system of claim 1 further including  
2 D. one or more second registers for holding elements of  $GF(2^m)$ ;  
3 E. one or more second multipliers for multiplying the contents of the first register  
4 by associated elements of  $GF(2^m)$  and supplying the products to update the one or more  
5 second registers; and  
6 F. one or more adders for adding the contents of the one or more second registers  
7 to the product produced by the first multiplier to produce a sum and supplying the sum to  
8 the first feedback means.

al  
1 16. (original) The system of claim 1 further including:  
2 D. a plurality of second multipliers each for multiplying the contents of the register  
3 by a multiplier constant that is a primitive element of  $GF(2^m)$ ; and  
4 E. a switch for selecting one of the plurality of second multipliers or the first multi-  
5 plier to produce the randomizer sequence.

1 17. (original) The system of claim 16 further including encryption means for encrypting a  
2 code word, the encryption means including:  
3 d. selection means for selecting an initial state for use in producing the random-  
4 izer sequence;  
5 e. means for combining the randomizer sequence with an ECC code word that is  
6 encoded in accordance with a given BCH code over  $GF(2^m)$ , the means pro-  
7 ducing a randomized code word; and  
8 f. means for producing a key associated with the selected the initial state.

1 18. (original) The system of claim 17 further including decryption means for using the  
2 key to reproduce the randomizer sequence and removing the randomizer sequence from  
3 the randomized code word to reproduce the ECC code word.

1 19. (original) The system of claim 18 wherein the selection means further selects the  
2 multiplier constant from a set of multiplier constants.

1 20. (original) The system of claim 15 further including encryption means for encrypting a  
2 code word, the encryption means including:

- 3 g. selection means for selecting an initial state for use in producing the random-  
4 izer sequence;
- 5 h. means for combining the randomizer sequence with an ECC code word that is  
6 encoded in accordance with a given BCH code over  $GF(2^m)$ , the means pro-  
7 ducing a randomized code word; and
- 8 i. means for producing a key associated with the selected the initial state.

ad 1 21. (original) The system of claim 20 further including decryption means for using the  
2 key to reproduce the randomizer sequence and removing the randomizer sequence from  
3 the randomized code word to reproduce the ECC code word.

1 22. (original) The system of claim 20 wherein the selection means further selects the  
2 multiplier constant from a set of multiplier constants.

1 23. (currently amended) A method for producing multiple-symbol randomizer sequences,  
2 the method including the steps of:

- 3 A. supplying an initial state to a first register;
- 4 B. producing a first product by multiplying the contents of the first register by a  
5 multiplier constant that is a primitive element of  $GF(2^m)$ ;
- 6 C. supplying the first product as
- 7 a. a next symbol of the randomizer sequence, and
- 8 b. an ~~to~~-update to the first register;
- 9 D. repeating steps A-C  $i$  times for  $i \leq 2^m - 2$ .

1 24. (currently amended) The method of claim 23 further including:

2 E.- in the step of supplying the initial state further including supplying an initial  
3 state to a second register;

4 F. in the step of producing a first product further including multiplying the con-  
5 tents of the second register by a multiplier constant that is an element of  
6  $GF(2^m)$  and adding the result to the first product; and

7 G. in the step of supplying the first product further including supplying the con-  
8 tents of the second register to update the first register.

1 25. (original) The method of claim 23 further including the step of selecting the initial  
2 state for the first register in order to produce a randomizer sequence for encryption.

1 26. (original) The method of claim 25 further including, in the step of selecting the initial  
2 state, selecting the initial state of the second register.

1 27. (original) The method of claim 26 further including the step of associating with each  
2 randomizer sequence a key that indicates the associated selected initial state.

1 28. (original) The method of claim 23 further including in the step of producing the first  
2 product further including selecting the multiplier constant to produce randomizer se-  
3 quences that are each a predetermined minimum distance from code words of a given  
4 BCH code.

1 29. (original) The method of claim 28 further including the step of detecting mis-  
2 synchronization by

3 a. combining the randomizer sequence with an ECC code word that is encoded in  
4 accordance with a given BCH code over  $GF(2^m)$ , to produce a randomized code word;

5 b. removing the randomizer sequence from the randomized code word to repro-  
6 duce the ECC code word; and

7 c. decoding the reproduced ECC code word and detecting a mis-synchronization  
8 if the number of errors in the reproduced ECC code word is greater than the number of  
9 errors that can be corrected by the given BCH code.

1 30. (original) The method of claim 28 wherein in the step of producing the first product  
2 further includes selecting the multiplier constant from a plurality of multiplier constants  
3 which each produce randomizer sequences that are respectively a predetermined mini-  
4 mum distance from code words of a given BCH code.

1 31. (original) The method of claim 30 further including the step of providing a key to se-  
2 lect the multiplier constants associated with a given randomizer sequence.

1 32. (original) The method of claim 23 further including

2 E. in the step of supplying the initial state supplying the initial state of one or  
3 more second registers;

4 F. in the step of producing the first product including the step of multiplying the  
5 contents of the first register in one or more second multipliers by associated primitive  
6 elements of  $GF(2^m)$  and supplying the products to update the one or more second regis-  
7 ters; and

8 G. in the step supplying further including the step of adding the contents of the  
9 one or more second registers to the product associated with the contents of the first reg-  
10 ister and supplying the sum as the next sequence symbol and to update the first register.

1 33. (original) The method of claim 23 further including in the step of producing the first  
2 product selecting a multiplier constant from a plurality of multiplier constants.

1 34. (original) The method of claim 23 further including a step of encrypting a code word  
2 by:

3 j. selecting an initial state for use in producing the randomizer sequence;

- 4 k. combining the randomizer sequence with an ECC code word that is encoded  
5 in accordance with a given BCH code over  $GF(2^m)$  to produce a randomized  
6 code word; and  
7 l. producing a key associated with the selected the initial state.

Al 1 35. (original) The method of claim 34 further including a step of decrypting the code  
2 word by using the key to reproduce the randomizer sequence and removing the random-  
3 izer sequence from the randomized code word to reproduce the ECC code word.

1 36. (original) The method of claim 34 wherein the step of selecting the initial state fur-  
2 ther includes selecting one or more multiplier constants.

---